Exhibit III-A: Matrix of Minimum Security Safeguards

Explanation: **This matrix is used to identify a minimum set of safeguards, by security level, which should be implemented to protect AISs, AIS facilities, and/or ITUs.[1]**

Justification for non-implementation of these safeguards should be based on the results of a formal risk analysis (and cost-benefit) study.

Directions: **Scan the Xs and Os beneath each security level designation. An "X" means that the security safeguard listed to the left is a requirement. An "O" means that the security safeguard is optional.**

Matrix of Minimum Security Safeguards				
	Security Level			
	Level 4 High Sensitivity/ Criticality, Nat'l Security	**Level 3** High Sensitivity/ Criticality	**Level 2** Moderate Sensitivity/ Criticality	**Level 1** Low Sensitivity/ Criticality
1. Ensure that a complete and current set of documentation exists for all operating systems.	X	X	X	X
2. Require use of current passwords and log-on codes to protect sensitive AIS data from unauthorized access.	X	X	X	O
3. Establish procedures to register and protect secrecy of passwords and log-on codes, including the use of a nonprint, nondisplay feature.	X	X	X	O
4. Limit the number of unsuccessful attempts to access an AIS or database.	X	X	X	O
5. Develop means whereby the user's authorization can be determined. (This may include answerback capability.)	X	X	X	O
6. Establish an automated audit trail capability to record user activity.	X	X	X	O
7. Implement methods, which may include the establishment of encryption, to secure data being transferred between two points.	X	X	O	O
8. Ensure that the operating system contains controls to prevent unauthorized access to the executive or control software system.	X	X	X	O
9. Ensure that the operating system contains controls that separate user and master modes of operations.	X	X	X	O
10. Record occurrences of nonroutine user or operator activity (such as unauthorized access attempts and operator overrides) and report to the organizational ISSO.	X	X	O	O

[1] OMB Circular A-130 requires formal risk analyses for sensitive AISs, AIS facilities, and ITUs. Required security safeguards may change as a result of the risk analysis.

Matrix of Minimum Security Safeguards				
	Security Level			
	Level 4 High Sensitivity/ Criticality, Nat'l Security	**Level 3** High Sensitivity/ Criticality	**Level 2** Moderate Sensitivity/ Criticality	**Level 1** Low Sensitivity/ Criticality
11. Ensure that the operating system provides methods to protect operational status and subsequent restart integrity during and after shutdown.	X	X	O	O
12. Install software feature(s) that will automatically lock out the terminal if it is not used for a predetermined period of lapsed inactive time, for a specified time after normal closing time, or if a password is not entered correctly after a specified number of times.	X	X	X	O
13. Ensure that the operating system contains controls to secure the transfer of data between all configuration devices.	X	O	O	O
14. Establish controls over the handling of sensitive data, including labeling materials and controlling the availability and flow of data.	X	X	X	O
15. Require that all sensitive material be stored in a secure location when not in use.	X	X	X	O
16. Dispose of unneeded sensitive hard copy documents and erase sensitive data from storage media in a manner which will prevent unauthorized use.	X	X	X	O
17. Prepare and maintain lists of persons authorized to access facilities and AISs processing sensitive data.	X	X	X	O
18. Establish procedures for controlling access to facilities and AISs processing sensitive data.	X	X	X	X
19. Furnish locks and other protective measures on doors and windows to prevent unauthorized access to computer and support areas.	X	X	X	X
20. Install emergency (panic) hardware on "Emergency Exit Only" doors. Ensure that emergency exits are appropriately marked.	X	X	X	X
21. Specify fire-rated walls, ceilings, and doors for construction of new computer facilities or modifications of existing facilities.	X	X	O	O
22. Install smoke and fire detection systems with alarms in the computer facility. When feasible, connect all alarms to a control alarm panel within the facility and to a manned guard station or fire station.	X	X	O	O
23. Install fire suppression equipment in the computer facility, which may include area sprinkler systems with protected control valves and/or fire extinguishers.	X	X	X	O
24. Provide emergency power shutdown controls to shut down AIS equipment and air conditionsing systems in the event of fire or other emergencies. Include protective covers for emergency controls to prevent accidental activation.	X	X	X	O

Matrix of Minimum Security Safeguards				
	Security Level			
	Level 4 High Sensitivity/ Criticality, Nat'l Security	**Level 3** High Sensitivity/ Criticality	**Level 2** Moderate Sensitivity/ Criticality	**Level 1** Low Sensitivity/ Criticality
25. Provide waterproof covers to protect computers and other electronic equipment from water damage.	**X**	**X**	**O**	**O**
26. Establish a fire emergency preparedness plan to include training of fire emergency response teams, development and testing of an evacuation plan, and on-site orientation visits for the local fire department.	**X**	**X**	**X**	**O**
27. Secure communication lines.	**X**	**X**	**X**	**O**
28. Conduct Tempest testing of operating system.	**X**	**O**	**O**	**O**
29. Ensure that all requirements of NSDD-145 (National Security Decision Directive) are met.	**X**	**O**	**O**	**O**
30. Establish detailed risk management program.	**X**	**X**	**X**	**O**
31. Establish Computer Systems Security Plans for sensitive systems.	**X**	**X**	**X**	**O**
32. Conduct formal risk analyses.	**X**	**X**	**X**	**O**
33. Establish employee security awareness and training programs.	**X**	**X**	**X**	**X**
34. Maintain accurate inventory of all hardware and software.	**X**	**X**	**X**	**X**
35. Establish security review and certification program.	**X**	**X**	**X**	**O**
36. Establish contingency plan.	**X**	**X**	**X**	**O**
37. Establish emergency power program.	**X**	**X**	**X**	**O**
38. Ensure that all personnel positions have been assigned security level designations.	**X**	**X**	**X**	**X**
39. Conduct periodic security level designation reviews.	**X**	**X**	**X**	**O**
40. Ensure that all personnel, including contractors, have received appropriate background investigations.	**X**	**X**	**X**	**O**
41. Maintain a list of all personnel, including contractors, who have been approved for 6C (High Risk Public Trust), 5C (Moderate Risk Public Trust), 4C (Top Secret, requiring special security considerations), 3C (Top Secret), and 2C (Secret or Confidential) risk level positions.	**X**	**X**	**O**	**O**